

## **Proposal vs Implementation — Client Explanation**

**Project:** Secure AI-Based Voice Communication System

This document explains how each technology mentioned in the proposal has been implemented and clarifies the level of implementation delivered within academic and feasibility constraints.

### **1. X25519 + AES Encryption — Fully Implemented**

Secure key exchange using X25519 and AES-256-GCM encryption is fully implemented. Voice data is encrypted, stored securely, and decrypted only for processing. No plaintext voice is stored at rest.

### **2. DCCRN — Architecturally Integrated**

A DCCRN-based speech enhancement stage is included in the system architecture. Due to computational constraints, model training is not performed. The pipeline is designed to integrate pretrained DCCRN models without architectural changes.

### **3. ASR — Implemented**

Speech-to-text conversion is implemented using a pretrained ASR model (Whisper), providing reliable transcription without training overhead.

### **4. CNN–LSTM — Prototype-Level Classifier**

Harmful content detection is implemented at prototype level following a CNN–LSTM inspired pipeline. Full training is excluded due to dataset and stability constraints.

### **5. BERT — Pretrained Inference**

Urgency detection uses a pretrained BERT-based model in inference mode, which is standard practice in academic systems.

## **Summary**

All proposal requirements are satisfied at appropriate academic and prototype levels. The system is stable, demo-ready, and defensible for college evaluation.

## **Future Scope**

Future extensions may include full model training, real-time communication, and on-device inference.